PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Appellant:	**Andrew Charles David HAY et al.**	Examiner:	Cao H. NGUYEN
Serial No.:	**09/931,657**	Art Unit:	2173
Filed:	August 16, 2001	Our Ref:	30006646-2 US B-4271 618992-5
For:	"SECURITY APPARATUS"	Date:	October 27, 2008
		Re:	***Appeal to the Board of Appeals***

BRIEF ON APPEAL

Commissioner for Patents

Sir:

This is an appeal from the non-final rejection dated May 27, 2008, for the above identified patent application. Appellant submits that this Appeal Brief is being timely filed because the Notice of Appeal was filed on August 27, 2008. The amount of $510.00 for the fee set forth in 37 C.F.R. 1.17(c) for submitting this Brief was paid previously in connection with the Brief filed in this case on March 6, 2008.

REAL PARTY IN INTEREST

The real party in interest to the present application is Hewlett-Packard Development Company, LP, a limited partnership established under the laws of the State of Texas and having a principal place of business at 20555 S.H. 249 Houston, TX 77070, U.S.A. (hereinafter "HPDC"). HPDC is a Texas limited partnership and is a wholly-owned affiliate of Hewlett-Packard Company, a Delaware Corporation, headquartered in Palo Alto, CA. The general or managing partner of HPDC is HPQ Holdings, LLC.

RELATED APPEALS AND INTERFERENCES

There are no other appeals or interferences related to the present application.

STATUS OF CLAIMS

Claims 1-17 are pending in this application, stand rejected, are the subject of this Appeal, and are reproduced in the accompanying appendix.

STATUS OF AMENDMENTS

No amendment after the last Action has been entered.

SUMMARY OF CLAIMED SUBJECT MATTER

Claim 1 of the present disclosure is directed to a security apparatus comprising means for representing to a user a plurality of components of a computer platform (501; Fig. 6; Paragraph [0061] of the present application as published); means for representing to the user interactions (502, Figs. 5 and 8, paragraphs [0060] and [0065]) among the plurality of components (Figs. 7a-14; Paragraphs [0062]-[0093]); and means for allowing the user to modify a security setting (Paragraphs [0067, 0069-0070], and [0081-0082]) associated with at least one of the plurality of components (Paragraphs [0095]-[0102]).

Claim 6 of the present disclosure is directed to a method for modifying the security status of a computer apparatus, the method comprising representing to a user a plurality of components of a computer platform (501; Fig. 6; Paragraph [0061]); representing to the user interactions (502, Figs. 5 and 8, paragraphs [0060] and [0065]) among the plurality of components (components of 501; Figs. 7a-14; Paragraphs [0062]-[0093]); and allowing the user to modify a security setting (Paragraphs [0067, 0069-0070], and [0081-0082]) associated with at least one of the plurality of components (Paragraphs [0095]-[0102]).

Claim 10 of the present disclosure is directed to a computer system, comprising a memory (22) to store computer-readable code; and a processor (21) operatively coupled to said memory and configured to implement said computer-readable code, said computer-readable code being configured to represent to a user a plurality of computer components (501; Fig. 6; Paragraph [0061]); represent to the user interactions (502, Figs. 5 and 8, paragraphs [0060] and [0065]) among the plurality of computer components (components of 501; Figs. 7a-14; Paragraphs [0062]-[0093]); and allow the user to modify a security setting (Paragraphs [0067,

0069-0070], and [0081-0082]) associated with at least one of the computer components (Paragraphs [0095]-[0102]).

Claim 14 of the present disclosure is directed to a method for modifying the security status of a computer component, the method comprising depicting a plurality of computer components (501; Fig. 6; Paragraph [0061]); depicting interactions (502, Figs. 5 and 8, paragraphs [0060] and [0065]) among the plurality of computer components (components of 501; Figs. 7a-14; Paragraphs [0062]-[0093]); and allowing modification of a security setting (Paragraphs [0067, 0069-0070], and [0081-0082]) associated with at least one of the computer components (Paragraphs [0095]-[0102]).

GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Issue 1: Whether claims 1-17 are patentable under 35 U.S.C. 103(a) over U.S. Patent No. 5,966,441 to Calamera (hereinafter "Calamera")in view of U.S. Patent No. 6,209,099 to Saunder et al. (hereinafter "Saunder").

ARGUMENT

Issue 1: Whether claims 1-17 are patentable under 35 U.S.C. 103(a) over U.S. Patent No. 5,966,441 to Calamera (hereinafter "Calamera") in view of U.S. Patent No. 6,209,099 to Saunders (hereinafter "Saunders").

In the final Office Action of May 27, 2008, the Examiner rejects claims 1-17 under 35 U.S.C. 103(a) as being unpatentable over Calamera in view of Saunders. In particular and with respect to claims 1 and 6, the Examiner asserts that Calamera discloses all elements but for security apparatus comprising means for representing to a user a plurality of components of a platform, alleges that Saunders teaches precisely this limitation, and opines that the skilled person would have found it obvious and would have been motivated to combine the two references and that such combination anticipates the claims. Appellants respectfully disagree.

At the outset, Appellants note that Calamera and Saunders are not analogous art, contrary to the clear mandate of MPEP §2141.01(a) that to rely on a reference under 35 U.S.C. 103, it must be analogous prior art:

> …a reference in a field different from that of applicant's endeavor

> may be reasonably pertinent if it is one which, because of the matter with which it deals, logically would have commended itself to an inventor's attention in considering his or her invention as a whole.
>
> ...
>
> While Patent Office classification of references and the cross-references in the official search notes of the class definitions are some evidence of "nonanalogy" or "analogy" respectively, the court has found "the similarities and differences in structure and function of the inventions to carry far greater weight."

Presently, Calamera is classified in U.S. Class 380/4: CRYPTOGRAPHY (equipment and processes which (a) conceal or obscure intelligible information by transforming such information so as to make the information unintelligible to a casual or unauthorized recipient, or (b) extract intelligible information from such a concealed representation, including breaking of unknown codes and messages), whereas Saunders is classified in U.S. Class 713/200: ELECTRICAL COMPUTERS AND DIGITAL PROCESSING SYSTEMS: SUPPORT (processes or apparatus for establishing original operating parameters or data for a computer or digital data processing system, such as, allocating extended or expanded memory, specifying device drivers, paths, files, buffers, disk management, etc…). Appellants submit that, as a matter of reason, a document directed to authenticating the software and hardware components of a system (Saunders) would not have logically commended itself to the attention of an inventor looking to implement a system for storing sensitive information in a cryptographically sensitive manner (Calamera). Looking at "the similarities and differences in structure and function of the inventions" only serves to prove this conclusion.

Addressing now the Examiner's incorrect interpretation of the cited art, Appellants note that Calamera teaches a technique for creating an autonomous network entity that stores sensitive information in a cryptographically secure manner. The autonomous entity comprises a data structure that encapsulates cryptographically-transformed information along with the inputs of a secret key used to reverse the transformation. Cryptographic storage of the sensitive information

and its reversible key within the encapsulated entity makes the entity autonomous and capable of transfer among computer platforms and their processes without compromising the security of the information.

However, and contrary to the Examiner's assertion, Calamera does not in fact disclose, suggest, or teach the presently claims means for representing to a user a plurality of components of a computer platform. The Examiner cites to col. 8 ll. 5-35 of Calamera as allegedly disclosing this claim feature, offering by way of explanation the comment: "…network-oriented component layer contains the underlying technology for creating encapsulated entity components that contain references to network resources located on computer networks." However, the careful reader will immediately discern that the language quoted by the Examiner contains no mention that a user is being presented with a representation of the interactions among the plurality of components as recited in Claim 1. Calamera teaches that these encapsulated entities manifest as visual objects to a user via a window environment to facilitate interactions between the user and the computer (c. 8, ll. 22-27 of Calamera). The only mention by Calamera of any interaction is the interaction of *network* components with *system software* routines (Column 8, ll. 29-32 of Calamera). Appellants submit that this clearly does not anticipate the presently claimed representing to the user interactions among a plurality of *components of a computer platform*.

Appellants note that the above discussion was previously presented to the Examiner, who dismissed it in the prior, final Action with the cryptic comment "… suggest represent to a user a plurality of computer components, represent to the user interactions among the plurality of computer components." In their previous Appeal Brief, Appellants showed - to the best of their understanding of the Examiner's comment - why this is not correct.

Appellants first noted that the figures of Calamera do not teach or suggest a user. Fig. 2 is a block diagram of a client computer, such as a personal computer, on which the invention may advantageously operate; Fig. 3 is a block diagram of the server computer of Fig. 1; Fig. 4 is a highly schematized block diagram of a layered component computing arrangement in accordance with the invention; and Fig. 5 is a schematic illustration of the interaction of a component, a software component layer and an operating system of the computer of Fig. 2.

The Examiner specifically cited to col. 8 ll. 17-24, where Calamera discloses "[t]he network-oriented component system which, when invoked, causes actions to take place that

enhance the ability of a user to interact with the computer to create encapsulated entities that contain references to network resources located on computer networks, such as the Internet." This certainly does not teach or suggest representing to the user interactions among a plurality of components of a computer platform. Something that may "enhance the ability of a user to interact with the computer" could not possibly be understood by one skilled in the art as encompassing "means for representing to the user interactions among the plurality of components." The language of Calamera cited by the Examiner further discloses that "This behavior of the system is brought about by the interaction of the network components with a series of system software routines associated with the operating system 420. These system routines, in turn, interact with the component architecture layer 430 to create the windows and graphical user interface elements" (c. 8, ll. 28-33 of Calamera). Appellants respectfully submit that this language also clearly does not teach or suggest "means for representing to the user interactions among the plurality of components" as recited in claim 1.

Appellants also do not agree with the Examiner that Calamera the claimed means for *allowing the user to modify a security setting* associated with at least one of the plurality of components. The Examiner asserts that this feature is disclosed by Calamera at co. 12 ll. 21-51, but all this portion discloses is that Calamera creates an autonomous network entity that stores sensitive information in a cryptographically secure manner. There is however nothing in the cited portion nor anywhere else in Calamera that could be understood by the skilled person as teaching that this autonomous network entity allows "the user to modify a security setting" as recited in Claim 1.

Appellants further respectfully disagree with the Examiner's interpretation of Saunders. The Examiner supports his contention that Saunders discloses the presently claimed security apparatus comprising means for representing to a user a plurality of components of a platform by citing to one single statement in the Abstract of Saunders: "The present invention concerns a secure data processing method and system in which *the user or operator of the system can trust that all of the software and hardware components of the system have been authenticated*." (Appellants note that the Examiner's citation to col. 5 ll. 53-67 is incorrect as there is in fact no fifth column in Saunders.) Appellants submit that the Examiner's interpretation of Saunders is simply untenable in view of the plain disclosure of the reference, which makes no mention of or

allusion to *representing* to a user a plurality of components of a platform. Saunders' method of *authenticating* to a user software and hardware components of a system (or platform) has no bearing whatsoever upon the presently claimed step of *representing* to a user a plurality of components of a platform.

In light of the preceding, Appellants submit that the Examiner's rejection must fail as a matter of law because the asserted references do not in fact anticipate a single claimed limitation.

Further to the above, Appellants respectfully submit that the Examiner's conclusions fall far short of the requirements for a proper 35 USC §103 rejection as set forth in the MPEP as well as the new *KSR v. Teleflex* Examination Guidelines of October 10, 2007.

The new Guidelines provide that "When making an obviousness rejection, Office personnel must therefore ensure that the written record includes findings of fact concerning the state of the art and the teachings of the references applied. In certain circumstances, it may also be important to include explicit findings as to how a person of ordinary skill would have understood prior art teachings, or what a person of ordinary skill would have known or could have done. Factual findings made by Office personnel are the necessary underpinnings to establish obviousness." There are in fact no such factual findings in the present Action, rather in their stead a slew of statements mischaracterizing the prior art and conclusory statements as to what the skilled person, according to the Examiner's opinion, would allegedly have done. The Examiner specific explanation that it would have been obvious to the skilled person "having the teachings of Calamera and Saunders before him at the time the invention was made, for creating a secure of a network component system of Calamera to include a secure data processing system by a user, as taught by Saunders" defies easy comprehension as well as common sense - the system of Calamera provides a framework within which autonomous entities encrypt data and are capable of being transferred among computer platforms and their processes without compromising the security of the information (Calamera Abstract). There is no reason the skilled person would want to add the encumbrance of platform authentication to a system that is designed to isolate the encrypted data from the platform in the first place - what practical purpose would this serve?

The Examiner's proffered motivation is equally devoid of merit: "One would have been motivated to make such a combination in order to build a trusted relationship between the

computing apparatus and its users, involves platform integrity checking; therefore, it would enable to provide certain types of communication or information to be trusted to differing degrees." As noted above, building a trusted relationship between the platforms and the user has absolutely no practical effect upon the stated purpose of Calamera - to store cryptographically encrypted information. After all, the very aim of Calamera is to isolate the information from the platforms. Furthermore, the alleged provision of different degrees of trust to different types of communication or information finds no support nor practical application in either reference - and the Examiner offers not one iota of argument that could prove otherwise.

The Guidelines further admonish that "Although a rejection need not be based on a teaching or suggestion to combine, a preferred search will be directed to finding references that provide such a teaching or suggestion if they exist." As discussed immediately above, the Examiner's proffered motivation clearly is not to be found even between the lines of the references.

The Guidelines further set forth that "Any obviousness rejection should include, either explicitly or implicitly in view of the prior art applied, an indication of the level of ordinary skill." No such indication, explicit or implicit, is to be found in the Examiner's Action.

Perhaps the most instructive portion of the Guidelines is the clear statement that "The key to supporting any rejection under 35 U.S.C. 103 is the clear articulation of the reason(s) why the claimed invention would have been obvious. The Supreme Court in KSR noted that the analysis supporting a rejection under 35 U.S.C. 103 should be made explicit. The Court quoting *In re Kahn* stated that " '[R]ejections on obviousness cannot be sustained by mere conclusory statements; instead, there must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness.' " Again, rather than offer articulated reasoning with some rational underpinning, the Examiner merely asserts a conclusion of obviousness.

These Guidelines do make clear that "the familiar teaching-suggestion-motivation (TSM) rationale" can still be employed by Examiners in making an obviousness rejection. However, the Examiner has not even mentioned where such teaching or suggestion are to be found in either of the cited references, and appears to have assumed a motivation that fails in the very face of reason.

In view of all of the preceding, Appellants respectfully submit that the prior art on record does not disclose each and every claimed limitation, that the references cannot in fact be combined as alleged by the Examiner, and that attempting such an unworkable combination would not in fact have been obvious to a person of skill in the art. For all of these reasons, Appellants respectfully request the Board to kindly consider the foregoing discussion and overturn the Examiner on Appeal.

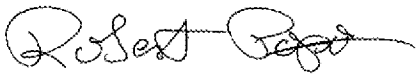
Appellants further respectfully submit that the foregoing discussion is equally probative of the novelty and nonobviousness of independent claims 10 and 14 and that of, at least in view of their dependencies, all pending dependent claims 2-5, 7-9, 11-13 and 15-17.

* * *

CONCLUSION

For the many reasons advanced above, Appellants respectfully contend that each pending claim is patentable and reversal of all rejections and allowance of the case is respectfully solicited.

Respectfully submitted,



Robert Popa
Attorney for Appellants
Reg. No. 43,010
LADAS & PARRY
5670 Wilshire Boulevard, Suite 2100
Los Angeles, California 90036
(323) 934-2300 voice
(323) 934-0202 facsimile
rpopa@la.ladas.com

CLAIMS APPENDIX

1. Security apparatus comprising:

means for representing to a user a plurality of components of a computer platform;

means for representing to the user interactions among the plurality of components; and

means for allowing the user to modify a security setting associated with at least one of the plurality of components.

2. Security apparatus according to claim 1, wherein the means for representing the plurality of components comprise:

means for representing software and/or hardware functionality of the computer platform.

3. Security apparatus according to claim 1, further comprising input means for allowing the user to interact with the modifying means to modify the security setting.

4. Security apparatus according to claim 1, further comprising means for providing possible modifications to the security setting.

5. Security apparatus according to claim 1, wherein a level of complexity of representing to the user the plurality of components is selectable by the user.

6. Method for modifying the security status of a computer apparatus, the method comprising:

representing to a user a plurality of components of a computer platform;

representing to the user interactions among the plurality of components; and

allowing the user to modify a security setting associated with at least one of the plurality of components.

7. The method according to claim 6, wherein representing the plurality of components comprises:

representing software and/or hardware functionality of the computer platform.

8. The method according to claim 6, further comprising:

presenting to the user possible modifications to the security setting.

9. The method according to claim 6, further comprising:

allowing the user to select a level of complexity of representing to the user the plurality of components.

10. A computer system, comprising:

a memory to store computer-readable code; and

a processor operatively coupled to said memory and configured to implement said computer-readable code, said computer-readable code being configured to:

represent to a user a plurality of computer components;

represent to the user interactions among the plurality of computer components; and

allow the user to modify a security setting associated with at least one of the computer components.

11. The computer system according to claim 10, wherein representing the plurality of computer components comprises:

representing software and/or hardware functionality of a computer.

12. The computer system according to claim 10, wherein the computer-readable code is further configured to:

present the user possible modifications to the security setting.

13. The computer system according to claim 10, wherein the computer-readable code is further configured to:

allow the user to select a level of complexity of representing to the user the plurality of computer components.

14. Method for modifying the security status of a computer component, the method comprising:

depicting a plurality of computer components;

depicting interactions among the plurality of computer components; and

allowing modification of a security setting associated with at least one of the computer components.

15. The method according to claim 14, wherein depicting the plurality of computer components comprises:

depicting software and/or hardware functionality of a computer.

16. The method according to claim 14, further comprising:

presenting possible modifications to the security setting associated with one or more of the computer components.

17. The method according to claim 14, further comprising:

allowing selection of a level of complexity for displaying the plurality of computer components.

EVIDENCE APPENDIX

There is no evidence submitted with the present Brief on Appeal.

RELATED PROCEEDINGS APPENDIX

There are no other appeals or interferences related to the present application.